

Notice of Allowability

Application No.

09/754,465

Examiner

Calvin L. Hewitt II

Applicant(s)

GRAY ET AL.

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to communication on 10-12-07.
2. ☒ The allowed claim(s) is/are 1, 3-5,39 and 40.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

Status of Claims

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Howard I. Sobelman, on 12 October 2007.

2. The Application has been amended as follows-

3. (currently amended) A method for authorizing a transaction, the method comprising:

completing shopping by a user at a merchant server;

initiating a transaction based on said shopping by receiving a request over a network at a wallet server, from said user, for payment authorization, wherein said request includes smartcard information and a selection of a financial institution;

prompting said user to physically interface a smartcard with a card reader system, wherein said smartcard comprises smartcard information including a digital certificate uniquely identifying said smartcard;

receiving said smartcard information from a computer coupled to said card reader system;

sending an authentication request for said transaction [to a security server of said selected financial institution] and said smartcard information by said wallet server to a security server of said selected financial institution;

receiving by the wallet server an authentication for said transaction from said security server;

completing an authorization form for said transaction by the wallet server and transmitting said authorization form to said merchant server;

requesting authorization of the authentication form from the security server by the merchant server;

authenticating said authorization form by said security server using said smartcard information; and,

receiving authorization form authentication from said security server by said merchant server, and said merchant server completing said transaction and debiting an account of said user.

39. (currently amended) A system for authorizing a transaction, the system comprising:

a wallet server comprising:

a first hardware interface [configured to receive] receiving an authorization request over a network from a user, for payment authorization, wherein said authorization request includes smartcard information from a smartcard and a selection of a financial institution;

a second hardware interface [configured to prompt] prompting said user to physically interface a smartcard with a card reader system, wherein said smartcard comprises smartcard information including a digital certificate uniquely identifying said smartcard;

memory receiving said smart card information from a computer coupled to said smart card system;

a processor [configured to send] sending an authentication request for said transaction [to a security server of said financial institution] and said smartcard information [by said wallet server] to a security server of said financial institution;

a first hardware module [configured to receive] receiving an authentication for said transaction from said security server;

a second hardware module [configured to complete] completing an authorization form for said transaction and transmitting said authorization form to said merchant server

said security server comprising:

a hardware module [configured to authenticate] authenticating said authorization form by [said security server] using said smartcard information; [and,]

said merchant server comprising:

a first processor requesting authorization of the authentication form from the security server;

a second processor [configured to receive] receiving authorization form authentication from said security server, completing said transaction and debiting an account of said user.

40. (currently amended) A computer-readable storage medium containing a set of instructions for a general purpose computer, wherein said set of instruction when [said set of instructions include] executed by the general purpose computer cause the computer to perform the steps of:

completing shopping by a user at a merchant server;

initiating a transaction based on said shopping by receiving a request over a network at a wallet server, from said user, for payment authorization, wherein said request includes smartcard information and a selection of a financial institution;

prompting said user to physically interface a smartcard with a card reader system, wherein said smartcard comprises smartcard information including a digital certificate uniquely identifying said smartcard;

receiving said smartcard information from a computer coupled to said card reader system;

sending an authentication request for said transaction [to a security server of said selected financial institution] and said smartcard information by said wallet server to a security server of said selected financial institution;

receiving by the wallet server an authentication for said transaction from said security server;

completing an authorization form for said transaction by the wallet server and transmitting said authorization form to said merchant server;

requesting authorization of the authentication form from the security server by the merchant server;

authenticating said authorization form by said security server using said smartcard information; and,

receiving authorization form authentication from said security server by said merchant server, and said merchant server completing said transaction and debiting an account of said user.

3. Claims 1-5, 39 and 40 have been examined.

4. Claims 1-5, 39 and 40 are allowed.

Reasons for Allowance

5. The present invention is directed to transaction security. Securing online transactions is old and well known. For example, secure protocols using cryptography such as SET and SSL are old and well known ("Secure transactions over the internet", Jim Montgomery, Communications News, Mar 1997). Daly (US 5,878,141) teaches a user sending an authorization request to a first server ('141, column 7, lines 1-46), the first server communicating with and receiving authorization from a second server for authorizing the user's financial

card ('141, column 8, lines 36-46), and prompting the user to enter card identification data ('141, column/line 8/61-9/7). Linehan (US 6,327,578) teaches a four party protocol wherein a bank or issuer gateway authenticates a user purchase by generating an authorization token and transmits the token to the user's wallet ('578, figure 3, item 310). The wallet in turn transmits the token to a merchant who submits the token to its bank for settlement with the issuer ('578, figure 3, items 312 and 314). Linehan also discloses a wallet server ('578, column/line 2/65-3/3). However, the prior art neither singly nor in combination teach or fairly suggest completing an authorization form for a transaction by a wallet server, transmitting said authorization form from the wallet server to a merchant server, the merchant server requesting authorization of the authentication form from the security server and authenticating the authorization form by the security server using said smartcard information.

Conclusion

6. Any comments considered necessary by Applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Art Unit: 3621

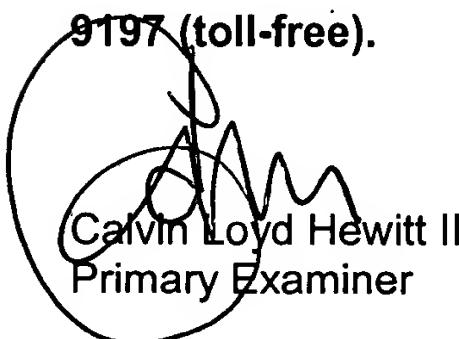
7. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Calvin Loyd Hewitt II whose telephone number is (571) 272-6709. The Examiner can normally be reached on Monday-Friday from 8:30 AM-5:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Fischer, can be reached at (571) 272-6779.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see

<http://pair-direct.uspto.gov/>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-

9197 (toll-free).



Calvin Loyd Hewitt II
Primary Examiner

October 15, 2007